

IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF VIRGINIA
ROANOKE DIVISION

IN THE MATTER OF THE SEARCH OF A
BLACK iPhone 6S SEIZED FROM SETH
ISAAH ADAMS ON MAY 29, 2020
CURRENTLY LOCATED AT DEA-
ROANOKE RESIDENT OFFICE

Case No. 7 : 20mj 75

**AFFIDAVIT IN SUPPORT OF AN
APPLICATION UNDER RULE 41 FOR A
WARRANT TO SEARCH AND SEIZE**

I, Ryan Sloan, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of property—an electronic device—which is currently in law enforcement possession, and the extraction from that property of electronically stored information described in Attachment B.

2. I am an “investigative or law enforcement officer” of the United States within the meaning of Section 2510(7) of Title 18 of the United States Code, and am empowered by law to conduct investigations of, and to make arrests for, offenses in violation of Title 18 and Title 21 of the United States Code.

3. I am a Task Force Officer with the Drug Enforcement Administration, and have been since September 2015. I have been employed by the Roanoke Police Department since October 2008. Prior to this DEA assignment, I spent 2 years assigned to the Patrol Bureau, 2 years assigned to the Street Investigations Unit and 3 years assigned to the Narcotics and Organized Crime Unit. During these assignments I have made narcotics arrests that have led to convictions at both the State and Federal levels. I have received training in the area of the

current investigation and detection of individuals involved in narcotics trafficking and related crimes. I have participated in the preparation and execution of numerous arrest and search warrants for criminal offenses involving controlled substances. I am familiar with the methods and patterns of illegal drug trafficking at both the street and wholesale level. I know from my training and experience how cellular devices are used to facilitate drug trafficking and related criminal activity, including the concealment of federal fugitives. I am further aware that the memory contents of these cellular devices often contain information of evidentiary value.

4. The facts in this affidavit come from my personal observations, and my training and experience, as well as information obtained from other law enforcement officers and in interviews with witnesses. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

IDENTIFICATION OF THE DEVICES TO BE EXAMINED

5. The property to be searched is a Black iPhone 6S seized from Seth Isaiah ADAMS in connection with his arrest in Mexico on May 29, 2020 (hereinafter the "Device"). The Device is currently at DEA-Roanoke, Resident Office, located at 105 Franklin RD., Suite 200, Roanoke, VA.

6. The applied-for warrant would authorize the forensic examination of the Device for the purpose of identifying electronically stored data particularly described in Attachment B.

PROBABLE CAUSE

7. The United States, including the Drug Enforcement Administration, is conducting an investigation of Seth Isaiah ADAMS, Checaura FAULKNER, and others regarding potential

violations of the federal criminal code; specifically, harboring or concealing a federal fugitive, as a principal or as an aider and abettor, in violation of 18 U.S.C. § 1071.

8. The current investigation relates to the prosecution of large-scale drug trafficker Monta JORDAN and his associates, several of whom have been or are being prosecuted in the Western District of Virginia. The scope of the investigation included JORDAN and his associates, one of whom was identified as Seth Isaiah ADAMS. Through a court-authorized wiretap during the course of the investigation, agents obtained ongoing, recorded conversations between JORDAN and ADAMS reflecting ADAMS' role as a drug trafficker in the organization.

9. JORDAN was charged federally in 2017 along with co-conspirator, Clifton MEYERS. A number of ADAMS' distributors were charged in and around August 2018, including Luis MENDOZA, a relative of a Hispanic source of supply in the JORDAN-ADAMS drug operation. ADAMS was charged in December 2019. As he was led from the courtroom following his federal sentencing hearing in this district on January 29, 2020, MENDOZA stated to your affiant, "Good luck finding Seth ADAMS."

10. ADAMS had existing state warrants for his arrest at the time of his federal indictment and was believed to be hiding in Mexico from as early as the arrest of his sub-distributors in the fall of 2018. On information and belief, it was widely known on the streets that ADAMS had left the area to avoid state and federal authorities. A source of information, SOI 1, stated during an interview in 2018 that ADAMS had fled to Mexico to avoid law enforcement pressure in Roanoke. Another source of information, SOI 2, made a similar statement during an interview in 2019. When asked about the source of this information, SOI 2 advised that ADAMS was posting pictures on social media depicting himself surrounded by

Latino females, in addition to hearing information about his location secondhand from ADAMS' associates.¹

11. Your affiant was aware of a personal connection between ADAMS and an individual named Checvara FAULKNER from as early as 2018. In July 2018, officers stopped a vehicle occupied by ADAMS, FAULKNER, and ADAMS's alleged sub-distributor, Antonio PALMER.² Because ADAMS had state warrants at the time of the stop, he was taken into custody and later released by the state court on pretrial bond. He subsequently failed to appear for state court proceedings and remained a fugitive until his arrest in Monterrey, Mexico on May 29, 2020.

12. FAULKNER showed signs of communicating with ADAMS in Mexico through a series of activities beginning in 2019. In August 2019, FAULKNER attempted to send a FedEx package to Nuevo Leon, Mexico, weighing approximately 85 pounds, containing what FAULKNER described as clothing. The package was addressed to a Hispanic resident of Nuevo Leon with no known connection to the Roanoke area. She paid for the postage in cash. FedEx advised FAULKNER that the package likely would not make it through Customs but FAULKER asked that it be shipped anyway.

13. In September 2019, FAULKNER terminated her employment with Carilion and obtained no new identifiable employment or other source of income.

¹ SOI 1 and SOI 2 have pending federal criminal charges relating to drug distribution.

² PALMER has since pleaded guilty to federal drug charges in a separate case.

14. Between September 2019 and November 2019, call detail records for FAULKNER indicate that she was placing calls to Mexican phone numbers, as well as to a domestic phone number associated with ADAMS.³

15. Notwithstanding her loss of employment, FAULKNER began depositing cash into her Freedom First bank account and withdrawing it on the same day, in the form of sequential money orders made payable to a single payee. On information and belief, FAULKNER has no similar history of money order purchases. For example, in September 2019, FAULKNER deposited approximately \$3305 in cash and immediately purchased four sequential money orders totaling \$3300 made payable to a single payee. In October 2019, FAULKNER deposited \$4505 in cash and immediately purchased five sequential money orders totaling \$4500 made payable to a different payee. The pattern continued until FAULKNER's most recent trip to Mexico in February 2020. In all, FAULKNER deposited more than \$29,000 in cash between September 2019 and February 2020, and withdrew the same amount over approximately 32 money orders, numbered sequentially in clusters for specific payees. The average value of each money order was between \$500 and \$1000, and it appears from FAULKNER's bank records that each money order was deposited into one or more accounts at Wells Fargo Bank.

16. FAULKNER began traveling to Mexico during this time frame. On or about November 28, 2019, FAULKNER flew to from Charlotte, North Carolina to Monterrey, Mexico

³ DEA Roanoke received a call from an anonymous tipster in or about March 2020. During the call, the tipster stated that FAULKNER was flying to Mexico to see ADAMS, and that ADAMS was continuing to ship drugs to Roanoke. The tipster further provided a phone number for ADAMS of 304-309-2091. From call detail records, your affiant was able to determine that FAULKNER placed and received calls from this number between September and November 2019, on the same phone number – 540-664-1175 – she was using during her most recent trip to see ADAMS in Mexico between February and May 2020. DEA-Roanoke has not identified the anonymous tipster.

on American Airlines, returning to the United States on December 3, 2019, on a separate ticket through United Airlines. She flew to Monterrey, Mexico again on February 17, 2020, approximately two weeks after her most recent money order purchase. She was scheduled to return to the United States on April 27, 2020 but was delayed.

17. The day prior to her scheduled departure, on April 26, 2020, FAULKNER posted on her Facebook page a photograph of herself with Seth ADAMS reclining next to her. A few days prior to that, she posted on her Facebook page a photograph of herself with the name “Seth” and hearts tattooed across one side of her chest.

18. FAULKNER returned to the United States from Monterrey, Mexico on May 29, 2020. Seth ADAMS drove her to the Monterrey airport and was arrested as she boarded the plane. He had the Device in his possession at the time of arrest, as well as a fake Texas driver’s license and the debit card for the Freedom First bank account through which FAULKNER had been purchasing the money orders referenced above. The debit card bears FAULKNER’s name. Bank records for FAULKNER’s Freedom First account indicate that cash withdrawals were made from this account in Mexico in April 2020.

18. Your affiant knows from training and experience that cellular phones are a commonly used tool for individuals engaged in drug distribution and related crime, including flight from justice. In addition to call and text communication records, an analysis of call patterns and other data can reveal criminal associations and the location of a target of an investigation at critical times. Individuals engaged in covert criminal activity also use phones to conceal the nature and extent of criminal activity, through the use of voice-over-internet protocol (VOIP), broadband internet services, and encrypted messaging apps. Often evidence of such communications must be accessed directly through the telephonic device.

TECHNICAL TERMS

19. Based on my training and experience, I use the following technical terms to convey the following meanings:

- a. Wireless telephone: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional “land line” telephones. A wireless telephone usually contains a “call log,” which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic “address books;” sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system (“GPS”) technology for determining the location of the device.
- b. Digital camera: A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable

storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media appurtenant to digital cameras can contain any digital data, including data unrelated to photographs or videos and photographs and other digital images downloaded from the Internet.

- c. IP Address: An Internet Protocol address (or simply “IP address”) is a unique numeric address used by computers on the Internet. An IP address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet, including a wireless telephone, must be assigned an IP address so that Internet traffic sent from and directed to that computer or wireless telephone may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses which may be unique to a particular device or location, while other computers have dynamic—that is, frequently changing—IP addresses that may be assigned to a computer or wireless telephone for short periods while such devices are being used in a particular geographic location or through a specific Internet service provider.
- d. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

20. Based on my training, experience, and research, I know that the Device has capabilities that allow it to serve as a wireless telephone, digital camera, portable media player, GPS navigation device, and that the Device is likely to contain other communications applications, including but not limited to social media and other communications applications such as Snapchat, Instagram, Twitter, What's App, Signal, Facebook, and Facebook Messenger. In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the Device, specific communications between users of the Device and/or third parties, and data and other information downloaded to or accessed through the Device.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

21. Based on my training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

22. There is probable cause to believe that things that were once stored on the Device may still be stored there, for at least the following reasons:

- e. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data

contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

- f. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer’s operating system may also keep a record of deleted data in a “swap” or “recovery” file.
- g. Wholly apart from user-generated files, computer storage media—in particular, computers’ internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory “swap” or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.
- h. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or “cache.”

23. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the Device was used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the Device because:

- i. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).
- j. Forensic evidence on a device can also indicate who has used or controlled the device. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence.
- k. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when, in connection with criminal activity under investigation.
- l. The process of identifying the exact electronically stored information on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.
- m. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

24. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit examination of the Device consistent

with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of each Device to human inspection in order to determine whether it is evidence described by the warrant.

25. *Manner of execution.* Because this warrant seeks only permission to examine a device already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

CONCLUSION

26. I submit that this affidavit supports probable cause for a search warrant authorizing the examination of the Device described in Attachment A to seek the items and other evidence described in Attachment B.

REQUEST FOR SEALING

27. It is respectfully requested that this Court issue an order sealing, until further order of the Court, all papers submitted in support of this application, including the application and search warrant. I believe that sealing this document is necessary because the warrant is relevant to targets who are unaware of the existing investigation. In my training and experience, I have learned that online criminals actively search for criminal affidavits and search warrants via the internet, and disseminate them to other online criminals as they deem appropriate, i.e., post them publicly online through the carding forums. Premature disclosure of the contents of this affidavit and related documents may have a significant and negative impact on the continuing investigation and may severely jeopardize its effectiveness.

Respectfully submitted,

/s/ Ryan Sloan

Ryan Sloan
Task Force Officer
Drug Enforcement Administration

Sworn and attested to telephonically.

Subscribed and sworn before me
on June 12, 2020:

Robert S. Ballou

UNITED STATES MAGISTRATE JUDGE
Robert S. Ballou